FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	44835
Nombre	Seguridad
Ciclo	Máster
Créditos ECTS	2.0
Curso académico	2023 - 2024

Titulación(es)

Titulación	Centro	Curso	Periodo
2234 - M.U. en Tecnol. Web,Computac. Nube y Aplicac. Móviles 17-V.1	Escuela Técnica Superior de Ingeniería	1	Primer cuatrimestre

Materias

Titulación	Materia	Caracter
2234 - M.U. en Tecnol. Web,Computac. Nube y Aplicac. Móviles 17-V.1	5 - Producción de software, seguridad y profesión	Obligatoria

Coordinación

Nombre	Departamento
PEÑA ORTIZ, RAÚL	240 - Informática

RESUMEN

La asignatura introducirá al alumno en los conceptos de la seguridad en recursos y aplicaciones web del tipo cliente-servidor en las que la comunicaciones se realizan a través de un canal inseguro, como es Internet. Este tipo de aplicaciones es muy amplio y la asignatura trata de recoger las diferentes opciones que aparecen en las aplicaciones web actuales y de analizar los problemas y soluciones de seguridad. El principal objetivo es proveer al alumno de los mecanismos necesarios para poder incluir la seguridad como un elemento fundamental dentro del desarrollo de aplicaciones web.

CONOCIMIENTOS PREVIOS

Relación con otras asignaturas de la misma titulación

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

Otros tipos de requisitos

Conocer las tecnologías de programación del lado del servidor.
Conocer las tecnologías de programación del lado del cliente

COMPETENCIAS

2234 - M.U. en Tecnol. Web,Computac. Nube y Aplicac. Móviles 17-V.1

- Que los/las estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- Que los/las estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- Que los/las estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- Que los/las estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
- Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.
- Capacidad para la elaboración, planificación, dirección, coordinación, gestión técnica y económica y la implantación de proyectos Web.
- Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología en el ejercicio profesional.
- Fomentar en contextos académicos y profesionales, el avance tecnológico, social o cultural dentro de una sociedad basada en el conocimiento y en el respeto a: a) los derechos fundamentales y de igualdad de oportunidades entre hombres y mujeres, b) los principios de igualdad de oportunidades y accesibilidad universal de las personas con discapacidad y c) los valores propios de una cultura de paz y de valores democráticos.
- Capacidad para evaluar el riesgo y los problemas de seguridad en sistemas y aplicaciones y adoptar medidas para mitigarlos en el ámbito de las tecnologías web, computación en la nube y aplicaciones móviles.

RESULTADOS DE APRENDIZAJE

- Especificar y completar tareas informáticas que son complejas, definidas de forma incompleta o poco familiares
- Describir y explicar técnicas y métodos aplicables a su particular área de estudio e identificar sus limitaciones
- Organizar su propio trabajo de forma independiente, demostrando iniciativa y ejerciendo responsabilidad personal
- Realizar búsquedas bibliográficas y revisiones usando bases de datos y otras fuentes de información
- Aprender y mejorar el rendimiento personal como la base para el aprendizaje a lo largo de la vida y el desarrollo profesional
- Comunicar de forma efectiva tanto verbalmente como a través de otros medios de comunicación a una variedad de audiencias y preferiblemente en un segundo lenguaje
- Apreciar las habilidades requeridas para trabajar con y liderar un equipo que puede estar compuesto por diferentes disciplinas y diferentes niveles de cualificación
- Evaluar el riesgo y problemas de seguridad de la información relevantes a su área de estudio
- Conocer las principales vulnerabilidades en las aplicaciones web.
- Implementar y evaluar mecanismos de seguridad en el servidor, en el cliente y en la aplicación
- Demostrar conciencia de la necesidad de una conducta profesional ética en informática.
- Capacidad para analizar los requisitos de un sistema web sobre la base de su funcionalidad, prestaciones, usabilidad, necesidades organizativas y seguridad.
- Capacidad para proyectar esos requisitos en soluciones eficientes y eficaces que tengan en cuenta las necesidades, características y expectativas de sus usuarios.
- Asegurar las bases de datos y servidores de aplicaciones que se utilizan como herramientas para la ejecución de aplicaciones web.
- Identificar y valorar las principales amenazas a la seguridad de las aplicaciones web y los fallos que comúnmente se cometen en su programación.
- Analiza y extraer conclusiones sobre los errores en la seguridad que han permitido una intrusión en los servidores web, y elaborar nuevas medidas de seguridad para prevenir futuros intentos de intrusión en los servidores web.

DESCRIPCIÓN DE CONTENIDOS

1. Vulnerabilidades en las aplicaciones web

Aplicaciones web y el coste de la seguridad.
Las vulnerabilidades más críticas en las aplicaciones web.
Guías y recomendaciones de seguridad.
Instalación y uso de una plataforma para pruebas de vulnerabilidad en aplicaciones web.

2. Seguridad en el servidor

Fundamentos del protocolo HTTP.
Mecanismos de Seguridad disponibles en HTTP .
Autenticación en servidores web.
Almacenes de claves, certificados y SSL.
Utilidades de seguridad en el servidor.

3. Seguridad en el cliente

Gestión de sesiones HTTP y Hijacking.
Gestión de Cookies e implicaciones para la seguridad.
Políticas de protección del mismo origen.
Scripts de sitio-cruzado (XSS).
Falsificación de petición en sitios cruzados.
Redirecciones no válidas.
Inyección de datos en la cara del cliente y referencias directas inseguras a recursos.
Herramientas de seguridad a nivel de cliente.null

4. Seguridad a nivel de la aplicación

Autenticación y control de acceso basado en roles y listas de control de acceso.
Validación de formularios: cliente y servidor.
Vulnerabilidades en la capa de datos: acceso a base de datos, inyección SQL, exposición de datos sensibles.
Políticas y buenas prácticas de configuración de los recursos de las aplicaciones web.
Herramientas de seguridad a nivel de aplicación.

VOLUMEN DE TRABAJO

ACTIVIDAD	Horas	% Presencial
Clases teórico-prácticas	20,00	100
Estudio y trabajo autónomo	22,00	0
Preparación de clases prácticas y de problemas	6,00	0
Resolución de cuestionarios on-line	2,00	0
TOTAL	**50,00**	

METODOLOGÍA DOCENTE

- Clase de teoría
- Resolución de problemas
- Aprendizaje orientado a proyectos

EVALUACIÓN

Los sistemas de evaluación usados en esta asignatura son:

SE1: Evaluación en línea y/o grado de participación

SE2: Evaluación de problemas, trabajos, informes y/o memorias

SE4: Evaluación presencial

SE6: Evaluación de las prácticas de laboratorio

- Primera convocatoria: 0.1*SE1+0.3*SE2+0.2*SE4+0.4*SE6

- Segunda convocatoria: 0.4*SE4+0.6*SE6

Las restricciones necesarias que se han de cumplir para que se apliquen los porcentajes indicados anteriormente son las siguientes:

- La nota de SE1, SE2 y SE6 tiene que ser mayor o igual a 5.

El sistema de calificaciones está especificado en el siguiente enlace:

http://www.uv.es/uvweb/universidad/es/estudios-postgrado/informacion-administrativa-postgrado/permanencia-calificaciones/calificaciones-1285897761928.html

La normativas aplicables se encuentran en el siguiente enlace:

http://www.uv.es/uvweb/universidad/es/estudios-grado/informacion-academica-administrativa/normativas/normativas-universidad-valencia-1285850677111.html

REFERENCIAS

Básicas

- Simson Garfinkel,Gene Spafford, Web Security, Privacy & Commerce, OReally. 2nd Edition. 2011
- Christoph Kern,Anita Kesavan,Neil Daswani. Foundations of Security: What Every Programmer Needs to Know. 2006. Apress
- Dustin, E., Rashka, J., & McDiarmid, D. "Quality Web Systems: Performance, Security, and Usability". 2002. Addison-Wesley Longman Publishing Co., Inc.
- The Open Web Application Security Project. "OWASP TOP 10: Los diez riesgos más críticos en Aplicaciones Web". 2017. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

Complementarias

- Aleksa Vukotic, James Goodwill. Apache Tomcat 7. Apress. 2011.
- Stuart McClure, Saumil Shah, Shreeraj Shah. Web hacking: attacks and defense. 2003